NMR experiment factors numbers with Gauss sums

Michael Mehring,[1] Klaus Müller,[2] Ilya Sh. Averbukh,[3] Wolfgang Merkel,[4] and Wolfgang P. Schleich[4]

[1] *Physikalisches Institut, Universität Stuttgart, D-70550 Stuttgart, Germany*
[2] *Physikalische Chemie, Universität Stuttgart, D-70550 Stuttgart, Germany*
[3] *Department of Chemical Physics, Weizmann Institute of Science, Rehovot 76100, Israel*
[4] *Abteilung für Quantenphysik, Universität Ulm, D-89081 Ulm, Germany*

(Dated: February 1, 2008)

We factor the number 157573 using an NMR implementation of Gauss sums.

PACS numbers: 03.67.Lx, 03.67.-a, 82.56.-b, 02.10.De

According to the legend[1] Karl Friedrich Gauss as a child was given by his teacher the problem of adding all integers up to a given number m. His elegant solution rearranges the terms of the series in a convenient way arriving at the result

$$\sum_{k=1}^{m} k = \frac{1}{2} m(m+1) \tag{1}$$

which depends quadratically on m. In his adult life Gauss revisited square dependencies in the context of number theory[2] when he calculated the sum of quadratic phase factors which today carry the name Gauss sums[3]. In this contribution we present the first implementation of a factorization algorithm [4, 5] based on Gauss sums[6] by factorizing the number $N = 157573$ using NMR techniques. It is intriguing that the physical realization relies on the sum formula Eq. (1).

Factorization of numbers into their prime factors is considered a hard non-polynomial problem[7] for classical computers. It was Shor [8] who proposed a quantum algorithm which can solve the problem on a quantum computer[9] with a tremendous speedup as compared to a classical computer. Vandersypen et al.[10] demonstrated in an NMR implementation of the Shor algorithm with seven qubits the factorization of the number $15 = 3 \cdot 5$.

Gauss sums are the discrete version of the Fresnel integrals[11] familiar from classical optics effects such as diffraction from a wedge or the Feynman formulation of quantum mechanics. Thus they are a sum rather than an integral over quadratic phase factors. Due to this discreteness Gauss sums have interesting periodicity properties which manifest themselves in the Talbot effect[12], fractional revivals[13] or curlicues[14]. Due to this periodicity property they not only play an important role in number theory but are also an ideal tool to factor numbers. Indeed several such Gauss sum factorization algorithms[4, 5, 15, 16, 17, 18] have been put forward. All these schemes capitalize on the periodicity properties but differ in their method of implementation ranging from a N-slit Young interferometer[15] via molecules[16] and wave packet dynamics[17] to chirped laser pulses interacting with atoms[4, 5, 18]. However, so far no experimental demonstration of this approach has been provided[19].

In the present paper we use NMR techniques to realize a rather special Gauss sum which brings out factors with a remarkable contrast even when only a few terms appear in the sum. We start by briefly summarizing the essential ingredients of our scheme. Since we do not employ entanglement yet, we still need exponential resources. Nevertheless, the quasi-random interference[20] contained in the Gauss sums allows us to work with only a few terms in the sum. In the experiment this advantageous feature translates into the need for a few pulses within a decay time of the system only. We then turn to the experiment and demonstrate the power of the scheme for a number with six digits, but emphasize that extensions to much larger numbers are within reach.

Our experiment implements the Gauss sum[21]

$$\mathcal{A}_N^{(M)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left[-2\pi i\, m^2 \frac{N}{\ell}\right], \tag{2}$$

with $M+1$ terms and N is the number to be factored. The argument ℓ with $1 \leq \ell \leq \sqrt{N}$ scans through all integers between 1 and $\sqrt{N}$ for possible factors.

The capability of the Gauss sum, Eq. (2), to factor numbers stems from the fact that for an integer factor q of N with $N = q \cdot r$ all phases in $\mathcal{A}_N^{(M)}$ are integer multiples of 2π. Consequently the terms add up constructively and yield $\mathcal{A}_N^{(M)}(q) = 1$ as shown in Fig. 1 by black dots. When ℓ is not a factor the quadratic phases oscillate rapidly with m and $\mathcal{A}_N^{(M)}$ takes on small values.

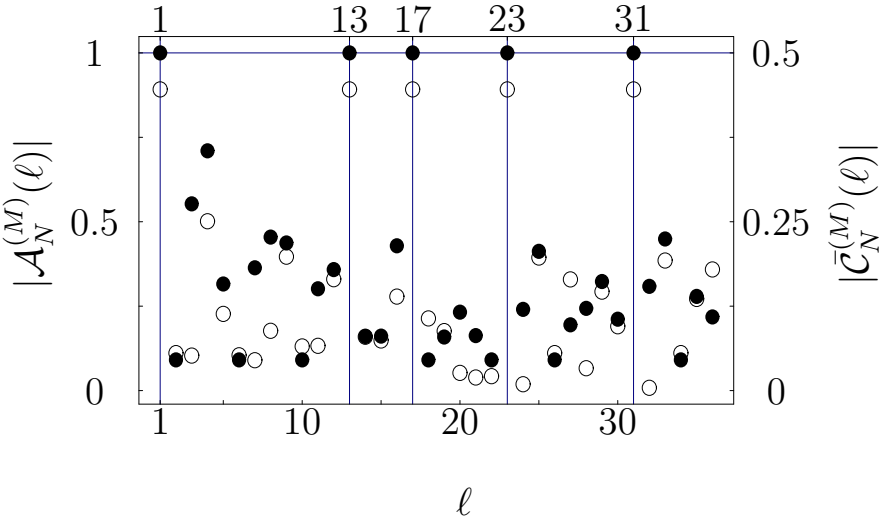

FIG. 1: Factorization interference pattern for $N = 157573 = 13 \cdot 17 \cdot 23 \cdot 31$ obtained from the Gauss sum $\mathcal{A}_N^{(M)}$ (black dots) and from the Gauss sum $\bar{\mathcal{C}}_N^{(M)}$ corresponding to damping (circles). In both cases already $M + 1 = 11$ terms are sufficient to clearly discriminate the factors from non-factors. Note the different scales for $\mathcal{A}_N^{(M)}$ and $\mathcal{C}_N^{(M)}$.

In this process of destructive interference the truncation parameter M plays a crucial role. Indeed, already a few terms in the sum are sufficient to discriminate factors from non-factors in the signal $|\mathcal{A}_N^{(M)}(\ell)|$. In order to analyze the dependence of this surprising feature on M we define the contrast[11] $\mathcal{V} \equiv (1 - a)/(1 + a)$ of the factorization interference pattern in complete analogy to classical optics where $a \equiv \sum_{\ell'=1}^{n_0} |A_N^{(M)}(\ell')|/n_0$ denotes the average value of the sum at the non-factors upto $\sqrt{N}$. Indeed, n_0 is the closest integer to $\sqrt{N}$ and the summation runs over all arguments ℓ' which are not factors of N. In Fig. 2 we show $\mathcal{V}$ for different values of N. Already a relatively small number of terms M results in good contrast of the signal.

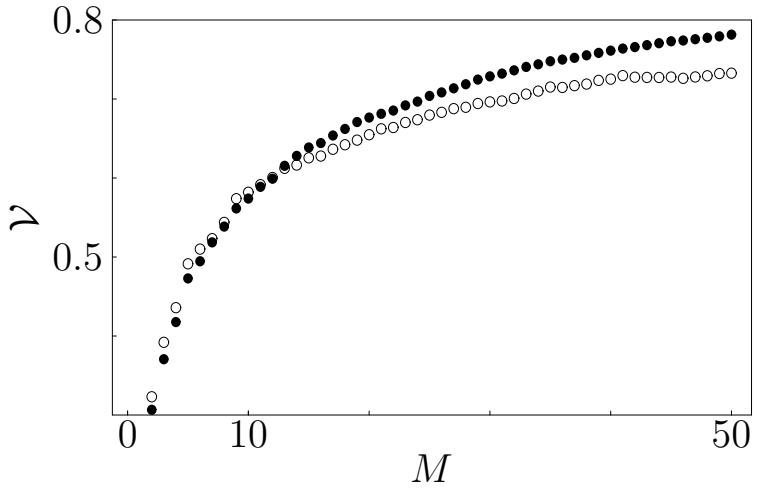

FIG. 2: The contrast $\mathcal{V}$ of the factorization interference pattern of Fig. 1 as a function of the number M of terms in the Gauss sum $\mathcal{A}_N^{(M)}$ for $N = 157573$ (circles) and $N = 4683359$ (black dots).

Next we address the complexity of our factorization scheme. To gain information on the factors of N we have to measure the signal $|\mathcal{A}_N^{(M)}(\ell)|$ for arguments ℓ belonging to the interval $[0, n_0]$. Since at most $\sqrt{N}$ data-points $\{\ell, |\mathcal{A}_N^{(M)}(\ell)|\}$ have to be acquired, we estimate the required resources as $\sqrt{N} = \exp[L/2]$ where $L = \log N$ is the number of digits of N. Although our scheme scales exponentially we profit from the small number of terms M necessary to distill the factors.

We now turn to our experimental realization of a Gauss sum. In the original proposal[4] the Gauss sum arises

through the time evolution of a two-level atom whose transition frequency increases linearly in time and which is driven by a train of laser pulses. In our experiment we subject an ensemble of spins $I = 1/2$ to a specific sequence of RF pulses as shown in Fig. 3. They lead to a sequence of signals which when summed represent a Gauss sum closely related to Eq. (2).

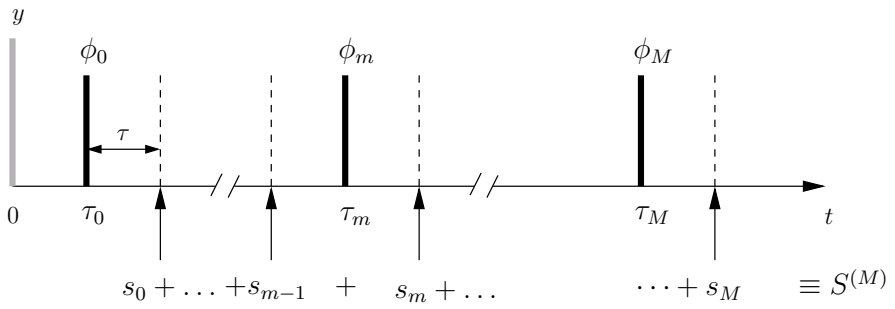

FIG. 3: NMR implementation of our factorization scheme using Gauss sums. The y-pulse which prepares the initial density matrix $\rho_{\rm in}$ is followed after a time τ by a pulse which imprints the phase ϕ_0 on the spins. This pulse is the first of a sequence of $M+1$ pulses each imprinting a different phase ϕ_m. At times $\tau_m + \tau \equiv (2m+1)\tau + \tau$ we measure the echo, that is the polarization s_m in x-direction and sum the echos s_m over all m to obtain $S^{(M)}$. In order to implement a Gauss sum the phases ϕ_m need to be proportional to the number N to be factored and have to increase linearly as a function of m since the spin dynamics expressed by s_m depends on the sum over all phases of the previous pulses.

In our experiment we use H_2O as an ensemble of protons with nuclear spin 1/2 in Boltzmann equilibrium at room temperature described by a density operator $\rho_B \equiv \mathbb{1}/2 - \epsilon\, I_z$, with the identity operator $\mathbb{1}$ and $0 < \epsilon \ll 1$. Throughout the paper we use the notation $I_j \equiv \sigma_j/2$ where σ_j are the familiar Pauli spin matrices.

Radio frequency pulses are applied at the Larmor frequency 400 MHz of the protons. Experiments were performed with a Varian Infinity Plus NMR spectrometer applying a cycle time of $t_c = 2\tau = 100\mu s$ and with relaxation time $T_2 \approx 200ms$. The pulse sequence shown in Fig. 3 is based on the Carr, Purcell, Meiboom and Gill (CPMG)-sequence[22, 23] which was proposed almost 50 years ago for measuring T_2 relaxation times in inhomogeneous fields. For our purpose we have modified this sequence such that the resulting evolution of the proton spins expressed by a sequence of echos which leads to the desired Gauss sum.

The pulse sequence consists of an initiating $\pi/2$-pulse in y-direction which creates the initial density matrix $\rho_{\rm in} \equiv \mathbb{1}/2 - \epsilon\, I_x$. This pulse is followed by a series of $M+1$ π-pulses with separation 2τ which are individually phase shifted with respect to the x-axis of the rotating frame by an angle ϕ_k[24, 25]. In the laboratory system the corresponding Hamiltonian reads

$$H(t) = \hbar\omega_0\, I_z + 2\pi\hbar \sum_{k=0}^{M} \delta(t - \tau_k) \cos(\omega\tau_k - \phi_k)\, I_x \tag{3}$$

where ω_0 and ω denote the frequencies of the transition and the driving field, respectively. The pulses act at times $\tau_k \equiv (2k+1)\tau$ and the phases ϕ_k will be chosen later in order to obtain a Gauss sum.

With the help of the identity

$$U_j(\alpha) \equiv \exp(-i\alpha I_j) = \cos(\alpha/2)\, \mathbb{1} - 2i\, \sin(\alpha/2)\, I_j \tag{4}$$

the Hamiltonian $\widetilde{H}$ within the rotating wave approximation, that is in the frame rotating with the frequency $\Delta\omega = \omega_0 - \omega$ takes the form

$$\widetilde{H} = \hbar\Delta\omega\, I_z + \pi\hbar \sum_{k=0}^{M} \delta(t - \tau_k)\, (\cos\phi_k\, I_x + \sin\phi_k\, I_y) \tag{5}$$

and the resulting time evolution operator

$$\mathcal{U}_k \equiv U_z(\Delta\omega\tau) U_z(\phi_k) U_x(\pi) U_z^\dagger(\phi_k) U_z(\Delta\omega\tau) \tag{6}$$

of the k-th cycle reflects the three stages shown in Fig. 3: (*i*) Free time evolution for the time τ followed by (*ii*) a π-pulse which imprints the phase ϕ_k, and (*iii*) another free time evolution during the time τ. The π-pulse eliminates

the effects of the free time evolution and ensures that the decoherence due to an inhomogeneous distribution of local fields is compensated by refocussing.

At times $\tau_m + \tau$ we measure the polarization

$$s_m \equiv \frac{\mathrm{Tr}\,(I_x \rho_m)}{\mathrm{Tr}\,(I_x \rho_{\mathrm{in}})} \tag{7}$$

in x-direction with $\rho_m \equiv \rho(\tau_m + \tau) = \mathcal{U}_m \rho_{\mathrm{in}} \mathcal{U}_m^\dagger$ where $\mathcal{U}_m \equiv \mathcal{U}(\tau_m + \tau) = \prod_{k=0}^{m} \mathcal{U}_k$ is the product of the time evolution operators $\mathcal{U}_k$ due to all previous pulses.

When we apply Eq. (4) to Eq. (6) we find

$$\mathcal{U}_k = (-i) \begin{pmatrix} 0 & \mathrm{e}^{-i\,\phi_k} \\ \mathrm{e}^{i\,\phi_k} & 0 \end{pmatrix} \tag{8}$$

which yields for the sum $S^{(M)} \equiv \sum_{m=0}^{M} s_m$ over the signals s_m given by Eq. (7) the expression

$$S^{(M)} = \sum_{m=0}^{M} \cos\left(\sum_{k=0}^{m} (-1)^k 2\phi_k \right). \tag{9}$$

Hence, the spin dynamics expressed by the signal s_m depends on its complete history, that is the phases of all previous pulses. In particular, they enter as an alternating sum. It is here that the sum Eq. (1) of the young Gauss comes into play. When we compare $S^{(M)}$ to the Gauss sum of Eq. (2) we recognize that for the choice

$$\phi_k = \begin{cases} (-1)^k (2k-1)\pi \frac{N}{\ell} & \text{for } k \geq 1 \\ 0 & \text{for } k = 0 \end{cases} \tag{10}$$

of the phases ϕ_k Eq. (9) takes the form

$$\frac{1}{M+1} S^{(M)} = \frac{1}{M+1} \sum_{m=0}^{M} \cos\left(2\pi\, m^2 \frac{N}{\ell} \right) \equiv \mathcal{C}_N^{(M)}(\ell) \tag{11}$$

with $\mathcal{C}_N^{(M)} = \mathrm{Re}\,\mathcal{A}_N^{(M)}$.

In Fig. 4 we display the results of our NMR implementation of our factorization scheme based on Gauss sums for $N = 157573 = 13 \cdot 17 \cdot 23 \cdot 31$. On the top we show the time evolution of the spin under the influence of the particular pulse sequence given by the Hamiltonian H and the phases ϕ_k defined by Eqs. (3) and (10), respectively. As a measure of the dynamics we show the echo signal s_m following from Eq. (7). For factors of N such as $\ell = 17$ the signal is constant. Consequently we find for the average $\mathcal{C}_N^{(M)}(\ell = 17)$ a value close to one as indicated in the bottom. However, for non-factors such as $\ell = 18$ the echo signal oscillates around 0 and leads to a rather small average value $\mathcal{C}_N^{(M)}(\ell = 18)$, shown by the arrow. We emphasize that due to the quasi-random interference of Gauss sums $M = 11$ terms are sufficient to discriminate factors from non-factors.

Although decoherence is not a limiting factor in our scheme it is still interesting to investigate its influence. We take incoherent processes into account phenomenologically by introducing a T_2 relaxation process and Eq. (9) is modified

$$\bar{\mathcal{C}}_N^{(M)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left(-m \frac{2\tau}{T_2} \right) \cos\left(2\pi\, m^2 \frac{N}{\ell} \right). \tag{12}$$

We find that even for an appreciable decay, that is for $2M\tau/T_2 = 2$ at the end of the sequence the pattern shown in Fig. 1 by circles looks almost identical to the one without decoherence indicated by black dots, except for the reduced scale of the signal strength. This result is surprising since the signal s_M at the end of the sequence has decayed to 13.5% of its initial value. Hence, decoherence does not significantly influence our ability to distinguish factors from non-factors.

In summary we have presented the first experimental implementation of a factorizing algorithm based on Gauss sums with an ensemble of single qubits. We have exemplified this technique factoring the number $N = 157573$. However, we claim that extensions to larger numbers are readily possible since our method capitalizes on the quasi-randomness of the phases of Gauss sums. As an outlook we factor in Fig. 5 the 24-digit number

$$N = 106288583786304618809830 7$$

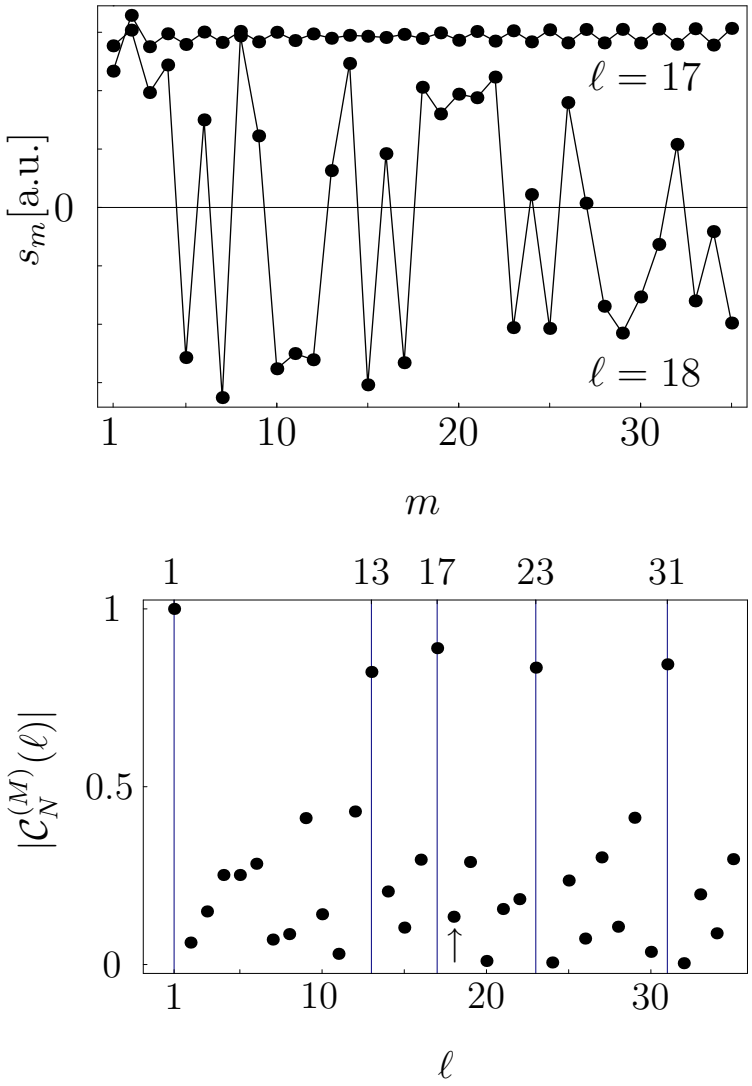

FIG. 4: Experimental realization of factoring $N = 157573 = 13 \cdot 17 \cdot 23 \cdot 31$ using the NMR implementation of the Gauss sum $\mathcal{C}_N^{(M)}$. In the top and bottom we depict the echo height s_m measured at times $\tau_m + \tau$ and the resulting average $\mathcal{C}_N^{(M)}$ for different trial factors ℓ, respectively. For factors such as $\ell = 17$ the signals s_m are approximately constant as a function of m with an average value $\mathcal{C}_N^{(M)}(17)$ close to unity. In contrast, for a non-factor such as $\ell = 18$ s_m oscillates around zero and when summed over m almost averages out as indicated by the arrow.

with only $M = 200$ pulses. Since in NMR it is possible to even have up to 10^4 pulses within the decay time T_2 several new questions emerge: (*i*) What is the optimal number M of terms in the Gauss sum, that is how many pulses are needed for a given N in order to discriminate factors from non-factors? (*ii*) How to overcome pulse errors? and (*iii*) how to employ entanglement in order to achieve a speed-up?

Obviously, the answers require a more detailed analysis. Therefore we can only speculate. However, our numerical experiments suggest a logarithmic dependence of M on N. In addition, pulse error correction techniques based on optimal control theory offer themselves. Finally, the entanglement of two and more spins might open a possibility to reduce the complexity.

We thank B. Girard, D. Haase, E. Lutz, H. Mack, H. Meier and G. G. Paulus for many fruitful discussions. Moreover, we are grateful to D. Suter for informing us about his experiment. We appreciate the support of the the Landesstiftung Baden-Württemberg in the framework of the Quantum Information Highway A8. The work of W. P. S. is also partially supported by the Max-Planck-Award.

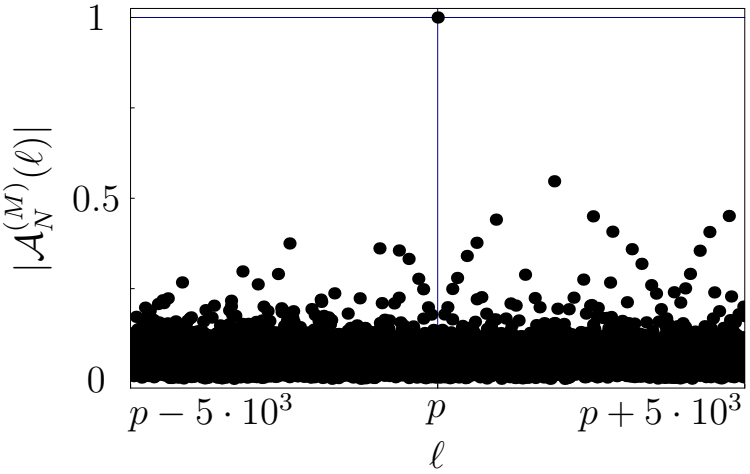

FIG. 5: Probing the limits of our factorization scheme. Factorization interference pattern for the 24-digit number $N = 106288583786304618809830 7 = p{\cdot}q$ obtained from a numerical simulation of the Gauss sum $\mathcal{A}_N^{(M)}$ in the immediate neighborhood of the prime factor $p = 790645490053$ for $M = 200$.

[1] See, for example J. Derbyshire, *Prime Obsession: Bernhard Riemann and the greatest unsolved problem in mathematics* (Penguin group, New York 2003).
[2] H. Davenport, *Multiplicative Number Theory* (Springer, New York, 1980).
[3] See, for example H. Maier and W. P. Schleich, *Prime Numbers 101: A Primer on Number Theory* (Wiley-VCH, New York, 2006).
[4] W. Merkel et al., Fortschritte der Physik **54**, 856 (2006).
[5] W. Merkel et al., Phys. Rev. A (2006), to be published.
[6] The discrete logarithm can be realized with the help of a quantum algorithm based on Gauss sums, see. for example W. van Dam and G. Seroussi, arXiv:quant-ph/0207131 (2002)
[7] S. Stenholm and K.-A. Suominen, *Quantum Approach to Informatics* (John Wiley , New York, 2005).
[8] P. Shor in: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, edited by S. Goldwasser (IEEE Computer Society Press, New York) pp. 124-134 (1994).
[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[10] L. M. K. Vandersypen et al., Nature **414**, 883 (2001).
[11] M. Born and E. Wolf, *Principles of Optics* (Pergamon Press, Oxford, 1993).
[12] See, for example M. Berry, I. Marzoli, and W. P. Schleich, Physics World **14**, 39 (2001).
[13] See, for example W. P. Schleich, *Quantum Optics in Phase Space*, (Wiley VCH, Berlin, 2001).
[14] M. V. Berry and J. Goldberg, Nonlinearity **1**, 1 (1988); M. V. Berry, Physica D **33**, 26 (1988).
[15] J. F. Clauser and J. P. Dowling Phys. Rev. A **53**, 4587 (1996).
[16] W. G. Harter, Phys. Rev. A **64**, 012312 (2001).
[17] H. Mack et al., phys. stat. sol. (b) **233**, 408 (2002); H. Mack et al., in: *Experimental Quantum Computation*, Eds. P. Mataloni and F. De Martini, (Elsevier, Amsterdam 2002).
[18] W. Merkel et al., Int. J. of Mod. Phys. B **20**, 1893 (2006).
[19] D. Suter has kindly informed us that he has implemented a related, but different NMR sequence leading to similar results (private communication).
[20] The interference of quadratic phases is at the heart of dynamical localization in the kicked rotor.
[21] This Gauss sum is related to the more familiar one

$$G(\ell, N) \equiv \sum_{m=0}^{N-1} \exp\left[2\pi i\, m^2 \frac{\ell}{N}\right]$$

by the Gauss reciprocity law[2, 3].
[22] H. Y. Carr and E. M. Purcell, Phys. Rev. **94**, 630 (1954).
[23] S. Meiboom and D. Gill, Rev. Sci. Inst. **29**, 688 (1958).
[24] W. S. Warren, D. P. Weitekamp, and A. Pines, J. Magn. Reson. **40**, 581-583 (1980).
[25] R. R. Ernst and G. Bodenhausen and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*, (Clarendon Press, Oxford, 1987)